Accessible Version

Office of Inspector General
U.S. Government Accountability Office
September 30, 2019

INFORMATION SECURITY
Review of GAO's Program and Practices for Fiscal Year 2018

Report Highlights

Objective

This report presents the OIG's assessment of GAO's compliance with Federal Information Security Modernization Act of 2014 (FISMA) requirements.

What OIG Found

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program for the information and systems that support their operations and assets, including those provided or managed by another agency or contractor. Although GAO, as a legislative branch agency, is not subject to FISMA, its management has chosen to use FISMA as a set of best practices for its information security program. GAO has defined an information security program that is generally aligned with FISMA, however the OIG identified several opportunities for GAO to improve the implementation of its information security program and to ensure alignment with federal best practices.

While GAO continues to make progress in developing its organizational capability for understanding and managing cybersecurity risk, it faces challenges in three areas. The design of GAO's enterprise risk management program is largely consistent with National Institute of Standards and Technology (NIST) guidance although GAO has not fully implemented controls in the areas of Risk Management Strategy, Risk Assessment, and Supply Chain Risk Management. Specifically,

- GAO has established an enterprise risk management (ERM) program that defines the organization's risk management strategy; however, GAO needs to better define its risk appetite, including risk tolerances.

- Risk has not been assessed on all GAO systems. Although GAO has established a program to assess system risk, it has not been fully implemented. The assessment process includes categorizing the impact level of the system and creating a system security plan, if required.

- GAO policy requires that specific Information Technology (IT) security and privacy requirements be included in all contracts and based on the particular nature of the IT services and the data requirements of the contract. However, the procedures that GAO developed for security and privacy requirements did not address NIST recommendations for ensuring contracts meet security requirements.

Additionally, GAO has generally established information protection policies that are consistent with federal best practices but has not consistently implemented these policies and procedures. For example, GAO regularly scans its environments to discover vulnerabilities such as

misconfigurations and missing patches. However, critical and high priority vulnerabilities were not always remediated in a timely fashion. Also, GAO policies call for establishing baseline configurations that can be used to configure machines securely and detect changes in the environment, but many were not documented.

The OIG also identified opportunities for GAO to improve disaster recovery planning. GAO did not conduct a disaster recovery plan test in fiscal year 2018, and one high-impact system did not have a contingency plan defined. Finally, GAO did not complete a business impact analysis which helps to inform contingency planning decisions.

This report is being released in summary form due to the sensitive nature of the subject matter.

What OIG Recommends

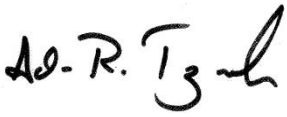
The OIG is making eight recommendations to strengthen GAO's information security program and practices. We recommend that GAO (1) finalize a key input to GAO's Enterprise Risk Management Strategy, specifically the risk appetite statement including risk tolerances; (2) review all entries in GAO's system inventory to determine if an impact assessment is needed and that assessments are performed as appropriate; (3) update standard operating procedures to ensure that standard contract language for security aligns with NIST recommendations as appropriate; (4) remediate identified vulnerabilities within prescribed time frames; (5) document and approve baseline configurations for all identified environments; (6) ensure that contingency planning testing accurately reflects the ability of GAO to recover mission critical systems in the event of a disaster; (7) document and approve a contingency plan for all high-impact systems; and (8) complete a business impact analysis for IT systems and update contingency plans where necessary to ensure that business needs are met in the event of a disaster. Management fully agreed with six of the eight findings and has identified actions taken or planned actions for the associated recommendations. For one of the findings (Rec. 4), GAO agreed with the finding but has not yet identified an action to be taken in response. For the remaining finding (Rec. 8), GAO disagreed with the finding but has stated that they will be taking action to address the associated recommendation.

Letter

September 30, 2019

To: Gene L. Dodaro
Comptroller General of the United States

From: Adam R. Trzeciak
Inspector General



Subject: Transmittal of Office of Inspector General's (OIG) Audit Report

Attached for your information is our final report, *Information Security: Review of GAO's Program and Practices for Fiscal Year 2018* (OIG-19-3). The audit objective was to evaluate the extent to which GAO has complied with Federal Information Security Modernization Act of 2014 (FISMA) requirements.

The report contains eight recommendations addressing areas that could be strengthened to improve GAO's information security program and practices. GAO fully agreed with six of the eights findings, and has identified actions taken or planned actions for the associated recommendations. For one of the findings GAO agreed with the finding but has not yet identified an action to be taken in response. For the remaining finding, GAO disagreed with the finding but has stated that it will be taking action to address the associated recommendation. The agency also provided technical comments that we incorporated, as appropriate. Management comments are included in appendix II of our report. Actions taken in response to our recommendations are expected to be reported to our office within 60 days. We are sending copies of this report to the other members of GAO's Executive Committee, Congressional Oversight Committees, Audit Advisory Committee, and other GAO managers, as appropriate. A summary of the report is also available on the GAO website at http://www.gao.gov/about/workforce/ig.html and https://www.oversight.gov/reports.

If you have questions about this report, please contact me at (202) 512-5748 or trzeciaka@gao.gov.

Attachment

Table of Contents

Table

Abbreviations

ACF	Alternate Computing Facility
ADF	Applied Research and Methods Data Facility
ARM	Applied Research and Methods
BIA	Business Impact Analysis
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
ISSG	Information Systems Security Group
ISTS	Information Systems and Technology Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
RMF	Risk Management Framework

Introduction

The U.S. Government Accountability Office (GAO), the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions.

To achieve its mission and goals, GAO relies extensively on information technology to fulfill its mission and support related administrative needs. The systems that GAO relies on perform functions such as, document management, workflow management, report publishing, and bid protest tracking.

As technology has advanced, GAO's dependence on information systems to carry out critical operations and to process, store, and share essential information has grown. Additionally, given GAO's extensive audit engagement portfolio which touches many sensitive government programs, the data that GAO maintains represents a significant store of information that needs to be protected from potential theft, loss, or misuse.

Strong information security controls reduce risks to information systems, the data they contain, and the people and processes they support. GAO systems must maintain effective information security controls to avoid being compromised, potentially resulting in damage to the organization, national security, or individual privacy.

GAO's Office of Inspector General (OIG) regularly assesses GAO's compliance with Federal Information Security Modernization Act of 2014[1] (FISMA) requirements. This report presents our assessment for Fiscal Year 2018.

Objective, Scope, and Methodology

We measured GAO's performance against select FISMA reporting metrics.[2] The FISMA reporting metrics we used were from the following five categories of controls: (1) risk management: (2) configuration management, (3) contingency planning, (4) security training, and (5) information system continuous monitoring. We selected these specific metrics, using a risk based approach, taking into account areas where GAO has previously experienced challenges. Areas that we did not review include, but are not limited to, access control, physical security, logging and monitoring, and incident response. We did not assess the maturity of GAO's information security against the reporting metrics in the categories above.

To assess GAO's performance, we analyzed the agency's information security policies, procedures, and guidance, interviewed staff in GAO's Information Systems and Technology Services (ISTS) and analyzed data and documentation we obtained from them. We also considered other security-related work in planning and performing our

[1]Pub. L. No. 113-283, Dec. 18, 2014.

[2]U.S. Department of Homeland Security, *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metric*s, (May 24, 2018).

audit, as appropriate. Additional information on our scope and methodology is presented in appendix I.

We conducted this performance audit from December 2018 through September 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Federal Laws and Guidance Establish a Framework for Executive Branch Agency Information Security Programs

Congress has long recognized the importance of ensuring the security of federal information systems. In 2002, Congress passed the Federal Information Security Management Act[3] (FISMA 2002) which laid out responsibilities for executive branch agencies, including requiring each agency to develop, document, and implement an agency wide information security program for the information and information systems that support the operations and assets of the agency, using a risk-based approach to information security management. The act also assigned to the National Institute of Standards and Technology (NIST) the responsibility for developing standards and guidelines that include minimum information security requirements. Additionally, the Office of Management and Budget (OMB) publishes guidance for executive branch agencies on implementing the NIST requirements.

Subsequently, to update FISMA 2002 and recognize changes that had occurred in the information security landscape, in 2014, Congress passed the Federal Information Security Modernization Act of 2014[4] (FISMA) which included additional provisions for executive branch agencies such as defining OMB and the Department of Homeland Security reporting requirements.

In a partnership with the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems, NIST developed a Risk Management Framework (RMF)[5] to improve information security, strengthen risk management processes, and encourage reciprocity among organizations. The RMF emphasizes cybersecurity risk management by promoting the development of security and privacy capabilities into information systems throughout the system development life cycle. The RMF does this by recommending organizations maintain situational awareness of the security and privacy posture of those systems on an ongoing basis through continuous

[3]FISMA 2002 was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, Dec. 17, 2002.

[4]The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[5]NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

monitoring processes; and by providing information to senior leaders and executives to facilitate decisions regarding the acceptance of risk to organizational operations and assets.

As a complement to the RMF, NIST also developed the Cybersecurity Framework[6] (CSF), which provides guidance to help organizations align policy requirements, business needs, and technological methodologies for cybersecurity risk management. The CSF is based on five core security functions:

- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect: Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.[7]
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

Each of the five core security functions is broken into categories that describe the activities which make up the core functions. These categories describe a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. Table 1 below includes examples of categories for each of the five core functions.

[6]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014).

[7]Cybersecurity events are cybersecurity changes that may have an impact on the organizational operations (including mission, capabilities, or reputation).

Table 1: Selected Cybersecurity Framework Core Functions, Categories and Descriptions

Identify	
Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Risk Assessment	The organization understands the cybersecurity risk to organizational operations, organizational assets, and individuals.
Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Protect	
Identity Management and Access Control	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Awareness and Training	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Information Protection Processes and Procedures	Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
Detect	
Security Continuous Monitoring	***The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.***
Respond	
Response Planning	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Communications	Response activities are coordinated with internal and external stakeholders.
Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Recover	
Recovery Planning	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.

Source: NIST Framework for Improving Critical Infrastructure Cybersecurity.

Although GAO, as a legislative branch agency, is not subject to FISMA, including NIST and OMB guidance, its management has chosen to use FISMA as the framework for its information security program. As such, GAO has aligned its security program with executive branch best practices, such as FISMA.

Prior Information Security Assessment

Our FISMA review for fiscal years 2016 and 2017[8] concluded that GAO had continued efforts to improve upon existing capabilities and strengthen information security controls, most notably in the core functions of Protect, Detect, and Respond. However, we reported that additional improvements were needed to help ensure that security is fully consistent with best practices. For example, GAO had established, but not yet fully implemented, its ability to manage cybersecurity risk to systems, people, assets, data, and capabilities. We also identified configuration management issues that resulted in the continued use of an unpatched, outdated computer operating system and increased risk to the confidentiality, integrity, and availability of GAO data and devices. Additionally, we identified weaknesses in GAO's information system components inventory that could adversely affect expedient tracking and reporting of hardware and software vulnerabilities. Lastly, we found that while GAO's critical business processes are heavily dependent upon its Information Technology (IT) resources, GAO had limited recovery capabilities for key information technology systems at its Alternate Computing Facility (ACF). These findings resulted in three recommendations to GAO which are still being addressed and remain open at this time.

Challenges Exist in GAO's Ability to Manage Cybersecurity Risk

While GAO continues to make progress in developing its organizational capability for understanding and managing cybersecurity risk, it faces challenges in three areas. The design of GAO's enterprise risk management program is largely consistent with NIST guidance although GAO has not fully implemented controls in the areas of Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management.

GAO's Has An Enterprise Risk Management Framework But A Key Element and Program Metrics Can Be Better Defined

GAO has established an enterprise risk management (ERM)[9] program that defines the organization's risk management strategy; however, there is a key program element that is not documented. According to NIST Special Publication (SP) 800-39, an organizational risk management strategy:

- addresses how organizations intend to assess, respond to, and monitor risk;
- makes explicit the specific assumptions, constraints, risk tolerances, and priorities or trade-offs used within organizations for making investment and operational decisions;
- addresses any strategic-level decisions and considerations on how senior leaders are to manage information security risk to organizational operations and assets, individuals, other organizations, and the nation;

[8]GAO, *Information Security: Review of GAO's Program and Practices for Fiscal Years 2016 and 2017*, OIG-18-4 (Washington, D.C.: July 17, 2018)

[9]OMB defines enterprise risk management as an Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.

- includes an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk response strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time;
- is informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.

GAO is in the process of implementing an ERM program that is in alignment with executive branch requirements such as OMB Circular A-123[10] which states that agencies should consult NIST special publications as part of their risk management strategy. GAO guidance generally aligns with NIST recommendations for a risk management program. According to NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, organizations should develop and document a risk assessment policy that addresses responsibilities for key roles. These roles include mission/business owners, chief information officers, chief information security officers, authorizing officials, and the risk executive.

As stated in its risk management policy, GAO management is responsible for determining appropriate risk responses based on impact and likelihood of the risk occurring. This GAO policy established a risk executive function that names the Chief Operating Officer and the Chief Financial Officer as GAO's Chief Risk Officers, charged with providing overall leadership for the ERM program. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. Additionally, the policy calls for creating a risk profile that reflects management's assessment of potential risks, current risk responses, and residual risk remaining after response actions had been taken.

While OMB does not require a risk appetite[11] and risk tolerance[12] document, NIST recommends a risk appetite statement. According to GAO, they intend to create a risk appetite document which would include risk tolerance measures. GAO has noted in its prior work that developing an agency risk appetite requires leadership involvement and discussion. The organization should develop a risk appetite statement and embed it in policies, procedures, decision limits, training, and communication, so that it is widely understood and used by the agency. However, GAO's risk appetite statement which identifies assumptions, constraints, risk tolerances, and priorities was not documented. Until GAO documents and communicates its risk appetite, including risk tolerances, the organization will be limited in effectively planning and implementing appropriate risk responses.

GAO's ERM policy also states that management must determine which risks require the design and implementation of internal control activities and that GAO should establish

[10]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (Washington, D.C.: July 15, 2016).

[11]According to OMB, risk appetite is the amount of risk an organization is willing to accept in pursuit of its mission. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives.

[12]According to OMB, risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

annual performance targets that reflect management's risk tolerance and assess performance quantitatively in four key areas – results, client, people, and internal operations. According to the policy, management and staff are to regularly monitor progress against planned performance targets, and develop plans to address identified risks.

With the exception of internal survey results on IT tools in GAO's Performance and Accountability Report, we did not see other performance targets or related monitoring in internal and external communications. This includes documents such as GAO's Congressional Budget Request, Performance Plan, and monthly updates to the Information Technology Investment Committee. In some cases, risk, cost, and schedule updates were presented, but either no performance targets were presented or those presented were not measureable or objective.

The lack of performance targets hampers GAO's ability to assess progress toward achieving its IT objectives and the incomplete implementation of GAO's ERM program limits the agency's ability to make informed decisions. We are not making a recommendation on the performance targets as we addressed ERM in our FISMA report for fiscal years 2016 and 2017 and were told that GAO is in the process of finalizing its ERM Program Plan and its implementation.

Improvements Needed to GAO's Systems Risk Assessment Process

GAO had not assessed risks for 20 systems out of the 115 systems listed within the inventory of ISTS's management portfolio. NIST SP 800-53[13] recommends that organizations assess and categorize the risk for information systems and components. A categorized information systems inventory is a first step in the system security planning activity. Categorization defines the impact to the organization or the nation based on the result of a loss of confidentiality, availability, or integrity. We identified 7 systems in the portfolio missing a risk assessment status, and 13 systems with the status "to be determined."

According to the Information Systems Security Group (ISSG), slightly less than half of the 115 systems are listed under the backlog category. According to ISSG, the backlog represents systems that have not yet undergone a full system security assessment which includes categorizing the impact level of the system and creating a system security plan. For some systems, ISSG has not determined whether an assessment is required. Other systems may require an assessment but have not had one.

ISTS staff members have stated that ongoing inventory improvement work is being completed as resources allow. Until then, GAO has reduced confidence that the authoritative systems list is accurate which increases the risk that management decisions based on that data will not be sufficiently informed.

[13]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

GAO Contracting Process Can Do More To Effectively Mitigate Supply Chain Risk

GAO's procedures did not ensure that organizations in their supply chain,[14] such as third-party partners and IT contractors, would implement measures that meet the objectives of GAO's cybersecurity program. NIST SP 800-53 Revision 4 recommends that organizations include language in their contracts that addresses information security requirements. This language should address security functional requirements; security strength requirements; security assurance requirements; security-related documentation requirements; requirements for protecting security-related documentation; description of the information system development environment and environment in which the system is intended to operate; and acceptance criteria.

Security functional requirements include security capabilities, security functions, and security mechanisms. Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls.

The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations defined in the organizational risk management strategy. Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement.

To ensure that IT contracts meet GAO security standards, GAO has established a policy requiring that specific IT security and privacy requirements must be included in all contracts and are based on the particular nature of the IT services and the data requirements of the contract. However, the procedures that GAO developed for security and privacy requirements did not address any of the six recommended elements from NIST. Specifically, one set of procedures references the protection of "sensitive information" but does not have specific requirements on how to do so. GAO defines sensitive information as "any information, the loss, misuse, or unauthorized access to, or modification of which, could adversely impact the interests of GAO in carrying out its programs or the privacy to which individuals are entitled" but the guidance only states that "Contracting Officers and the Program Offices they support must comply with the policy regarding protection of sensitive information discussed in applicable directives, and this chapter in the award of contracts for GAO." The only specific step required by contractors

[14]According to NIST, an organization's supply chain includes systems, services, components, and processes to create, maintain, and retire an organization's information systems. Examples include development environments, individuals who are working within the organization's facilities, and logistics for the transport of information systems and components. These elements of the supply chain infrastructure may be provided by the organization itself, a system integrator, or external service provider.

is to require a non-disclosure agreement if they have access to sensitive information. Until GAO takes steps to ensure that contracts contain language sufficient to define information security requirements when appropriate, there is an increased risk that contractors and suppliers will not meet information security requirements.

GAO Can Do More to Improve Safeguards for System Protection

GAO has generally established information protection policies that are consistent with federal best practices but has not consistently implemented these policies and procedures. For example, GAO has established policies and procedures to mandate that vulnerabilities are patched in a timely manner but we found that thousands of high and critical vulnerabilities had not been patched. Similarly, while GAO policies call for establishing baseline configurations that can be used to configure machines securely and detect changes in the environment, 19 out of 47 environments did not have baselines documented. GAO has established an Information Security Continuous Monitoring strategy which aligns with NIST guidance and would help identify needed information security controls if implemented effectively.

Critical and High Priority Vulnerabilities Were Not Always Remediated in a Timely Fashion

GAO regularly scans its environments to discover vulnerabilities such as misconfigurations and missing patches. However, critical and high priority vulnerabilities were not always remediated in a timely fashion. According to NIST SP 800-53 Revision 4, organizations should regularly scan for information systems vulnerabilities and ensure that they are corrected in a timely manner. NIST SP 800-53 Revision 4 also states that organizations should identify information systems affected by potential vulnerabilities, employing automated scanning tools and report this information to designated organizational personnel with information security responsibilities. To assess the risk that vulnerabilities are exploited by malicious actors, organizations should take advantage of available resources such as the Common Vulnerabilities and Exposures[15] (CVE) database in remediating flaws discovered in organizational information systems.

GAO routinely scans network, server and workstation environments and scan results are delivered monthly to staff responsible for reviewing, identifying, and tracking mitigation of vulnerabilities. As GAO has not independently assessed and prioritized discovered vulnerabilities, we reviewed the Common Vulnerability Scoring System[16] (CVSS) score for those vulnerabilities discovered during GAO's September 2018 scanning cycle. We

[15]Common Vulnerabilities and Exposures (CVE) is a list of common identifiers for publicly known cybersecurity vulnerabilities. Use of CVE Entries, which are assigned by CVE Numbering Authorities from around the world, ensures confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables automated data exchange.

[16]According to NIST, the Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and calculation of the severity of vulnerabilities discovered on agency systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

identified over 4,000 high or critical vulnerabilities (having a CVSS of High (7.0-8.9) or Critical (9.0-10.0), which had been unmitigated for over 90 days.

According to an ISTS staff member who works on vulnerability management, a lack of resources is preventing it from remediating the issues identified in a timely manner. However, ISTS has stated that the risk of exploitation for many of the vulnerabilities is low because they are not directly exposed to the internet. GAO has designed a series of controls aimed at preventing intruders from accessing internal systems; these include network monitoring, content filtering, and other intrusion prevention systems. Compensating controls, such as these, can help mitigate the risk from vulnerable systems, but an attacker who bypasses external network protections, whether from within the organization or through a phishing attempt, could potentially exploit GAO systems with unmitigated vulnerabilities. As GAO preventative phishing[17] exercises have shown, some employees fall for fake emails. Consequently, the risk remains that network users may unknowingly download malicious content that could exploit vulnerabilities from inside the GAO network.

GAO Has Not Documented Baseline Configurations for All Systems

GAO has documented baseline configurations for many of its environments but has not yet completed or started the process for others. NIST SP 800-53 Revision 4 recommends that organizations establish and document baseline configuration settings for information technology products. Baseline configuration settings are a set of common secure configurations for an information system, or portion of a system, that have been formally reviewed and agreed upon at a given point in time, and which can be changed only through change control procedures. Common secure configurations provide recognized, standardized, and established benchmarks that define secure configuration settings and instructions for configuring those information system components.

GAO procedures call for configuration baselines to be reviewed annually with quarterly check-ins to see if there are any changes that need to be made. For example, if a vendor introduces new configuration options it may be necessary to update the baseline configuration with new secure settings. Of the 47 listed technologies GAO identified, 19 configurations were not yet completed. Specifically, four of the baselines had been written but were awaiting signature or otherwise under review, seven were assigned to a subject matter expert and were under construction, and eight were listed as “planned” and had not yet begun.

According to ISTS, new systems that come online at GAO have baseline configurations developed before being placed in production. Still, baseline configurations for technologies that have already been deployed have not been a priority. Until GAO completes its baseline configurations, the agency is at increased risk of systems being configured insecurely which could lead to system breaches.

[17]Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or directs them to download malicious software.

System Changes Were Not Effectively Reviewed For Security Impacts

GAO has generally developed policies and procedures for ensuring that configuration changes are appropriately reviewed and approved before deployment but has not implemented those procedures consistently. NIST SP 800-53 Revision 4 recommends that organizations determine the types of changes to the information system that require review and conduct security impact analyses on those changes. Security impact analyses include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. These analyses may include reviewing system design documentation to understand control implementation and how specific changes might affect the controls. GAO policies and procedures are generally consistent with this NIST guidance including documenting what kinds of changes need security review and who is responsible for approving these changes. Specifically, GAO change control policy identifies three types of changes that need to be reviewed by the Change Control Board—Normal, Normal-Time Critical, and Emergency. Further, the policy states that these changes must be reviewed by a member of the security group for potential security impacts before Change Control Board approval is complete.

Implementation of these policies has been inconsistent. We found that 14 of the 37 changes listed as Emergency or Time Critical were not approved by an appropriate security person. As a result, changes to GAO's production environment were made without being reviewed by an appropriate security team member for security impacts. This finding is consistent with GAO's 2018 Financial Statement Audit, Management Letter comment. Consequently, we are not making a separate recommendation to address this issue. Until GAO consistently implements its review process GAO will be at an increased risk that changes will negatively impact the security of its computing environment.

GAO Implemented An Effective Awareness And Training Program

GAO has established a security awareness training program that aligns with NIST recommendations and meets agency goals. NIST SP 800-53 Revision 4 recommends that organizations provide basic security awareness training to information system users and if an organization chooses to supplement its security awareness training with practical exercises, it also recommend that organizations simulate actual attacks which could impact the agency. NIST SP 800-53 Revision 4 also recommends that security awareness training include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

To this end, GAO's security awareness training program met its completion goals and ensured that all individuals with network access received security awareness training in FY 2018. Additionally, GAO routinely distributed practical exercises for users in the form of phishing exercises. Specifically, the phishing exercise was designed to enable staff to recognize fraudulent messages disguised as legitimate e-mail messages. A malicious phishing attack attempts to trick the recipient into responding – by clicking a link, opening an attachment, or directly providing sensitive information. Furthermore, consistent with NIST guidance, GAO reviewed the results of these exercises and planned supplemental education for the user population accordingly. Supplemental education was in the form of communications to users about the results of the exercise or additional information provided to users who clicked on the link about likely indicators that a message may be fraudulent.

Opportunities Exist To Improve GAO's Disaster Recovery Planning

In the past, we have reported that GAO had not always ensured that systems could be recovered in the event of a significant disaster. GAO has taken some steps to plan for contingencies, but improvements are needed such as conducting contingency plan testing, annually including mission critical systems, ensuring that GAO's contingency planning covers all systems, and completing its business impact analysis.

Improvements Needed to GAO Recovery Plan Testing

GAO needs to improve recovery plan testing efforts to ensure that critical systems are available in the event of a disaster. NIST SP 800-34 Revision 1 recommends that agencies regularly test their information system contingency plans and that the tests be commensurate with system risk. Testing events assist organizations in determining the plan's effectiveness, and helps to ensure that all personnel know what their roles are in the conduct of each information system plan.

GAO did not conduct a test of contingency planning for GAO systems in fiscal year 2018. Until GAO successfully tests its ability to restore mission critical applications using its unified disaster recovery plan,[18] there is an increased risk that critical applications will not be available as needed following a disaster.

One High Impact System Did Not Have An Information System Contingency Plan

A contingency plan was not prepared as required for one GAO high impact system. NIST SP 800-53 Revision 4 states that contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for business functions and that contingency planning should address both information system restoration and implementation of alternative processes when systems are compromised. GAO Order 510.2, GAO Information Systems Security , states that GAO shall develop and maintain plans and procedures to ensure continuity of operations for GAO information systems.

The Applied Research and Methods Data Facility (ADF) did not have a contingency plan as required. The ADF is a system at GAO which processes sensitive data that requires information security controls consistent with a high-impact system[19] due to the sensitivity of data from other federal agencies that is processed there. While there are memoranda outlining steps that will be taken in the event of a disaster, the steps that would be taken to

[18]GAO does not maintain individual information systems contingency plans but instead has a disaster recovery plan that is intended to cover all systems in the event of a disaster which causes a loss of the primary computing facility.

[19]According to NIST Federal Information Process Standards Publication 199, impact is considered high when the loss of confidentiality, integrity, or availability for a system could be expected to potentially prevent the organization from performing one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

recover the system following a disaster are not well defined. According to ADF administrators, a variety of factors including recent organizational changes and lack of prioritization have prevented a contingency plan from being developed. Until GAO develops a contingency plan for this system, there is an increased risk that critical data will not be available to mission teams as needed following a disaster.

Contingency Planning Business Impact Analysis Has Not Been Fully Completed

GAO has not yet completed a business impact analysis to support contingency planning decisions. NIST 800-34 states that conducting a business impact analysis (BIA) is a key step to implementing contingency planning controls which help to identify recovery priorities and resource requirements. The purpose of a BIA is to correlate the system with the critical mission and business services provided, and based on that information, characterize the consequences of a disruption. The organization can use the BIA results to determine contingency planning requirements and priorities.

The official who coordinates development of GAO's Continuity of Operations Plan (COOP) indicated that GAO's COOP process is still maturing. This official also stated that during the initial COOP development process, business groups across GAO were consulted, however a BIA had not been developed. According to this official, the next opportunity to develop a business impact analysis would be in 2020 during the next planned COOP review. Without an appropriate business impact analysis, GAO increases the risk that it will not have correctly identified critical data that must be recovered in the event of a disaster.

Conclusions

GAO's mission requires it to collect and store data on a variety of government programs which makes it an attractive target for malicious actors. Security threats continue to evolve and become more sophisticated. Further, the speed at which new attack techniques become widely available, even to unsophisticated threat actors, underscores the need for GAO to continually improve its information security program. Generally, GAO has established policies and procedures that are consistent with a NIST aligned security program and has several initiatives underway to improve the security of its environment.

However, we identified areas of improvement that would help GAO better identify risks and ensure the security of the computing environment. As we had previously reported, GAO has an enterprise-wide risk management program but a key element can be better defined. Impact assessments had not been completed for all systems. Further, its contracting process does not ensure that third parties with access to sensitive GAO data protect it effectively. GAO action to correct these issues will help complete the data used to make risk-based decisions and decreased the risk of decisions not reflecting the actual operating environment.

In addition to improvements in risk management, we also identified opportunities for GAO to better protect its systems. Specifically, vulnerabilities are not being remediated in a timely manner with many of the outstanding vulnerabilities being high or critical impact. While compensating controls can help reduce the risk, the severity of the vulnerabilities leaves weaknesses in the system that can be exploited. Also, GAO has not documented

baseline configurations for all existing environments, a key to ensuring that systems are configured securely and consistently. GAO has opportunities to improve its disaster recovery program. In our prior report we found that GAO lacked the capacity to implement its existing recovery plan. In FY 2018, we found that contingency plan testing did not occur. Further, the existing contingency plan does not cover all systems; specifically a high-impact system used for processing sensitive external agency data and does not have a completed business impact analysis to inform contingency planning decisions and assumptions. It is important that GAO take continued steps to demonstrate its ability to recover from a disaster to reduce the risk that key systems or functionality will not be available.

Recommendations for Executive Action

We recommend that the Comptroller General direct the Chief Administrative Officer to take the following action:

1. *In order to ensure a complete and actionable cybersecurity risk management program, finalize a key input to GAO's Enterprise Risk Management Strategy, specifically the risk appetite statement including risk tolerances.*

We recommend that the Comptroller General direct the Chief Information Officer to take the following six actions:

2. *Ensure that all entries in GAO's system inventory have been reviewed to determine if an impact assessment is needed and that assessments are performed as appropriate.*
3. *Update standard operating procedures to ensure that standard contract language for security aligns with NIST recommendations as appropriate.*
4. *Take steps to ensure that identified vulnerabilities are remediated within prescribed time frames.*
5. *Ensure that baseline configurations for all identified environments have been documented and approved.*
6. *Ensure that contingency planning testing accurately reflects the ability of GAO to recover mission critical systems in the event of a disaster.*
7. *Document and approve a contingency plan for the ARM Data Facility.*

We recommend that the Comptroller General direct the Managing Director, Infrastructure Operations to take the following action:

8. *Complete business impact analysis for IT systems and update contingency plans where necessary to ensure that business needs are met in the event of a disaster.*

Agency Comments and Our Evaluation

The Inspector General provided GAO with a draft of this report for review and comment. GAO provided written comments, which are reprinted in appendix II. Management fully agreed with six of the eight findings and has identified actions taken or planned actions for the associated recommendations. For the two remaining findings, GAO either agreed with the finding but stated that no additional efforts are needed to address the finding (Rec. 4), or disagreed with the finding, (Rec. 8) citing an internal process that was not documented nor discussed with the OIG during fieldwork.

With regards to timely remediation of vulnerabilities, GAO agreed with the need to reduce risks to its systems, and committed to achieving the goal of ensuring that systems are protected from compromise but indicated that its current approach to vulnerability management is sufficient and no additional action is planned. Specifically, in response to Rec. 4, which states that GAO should “take steps to ensure that identified vulnerabilities are remediated within prescribed time frames”, GAO stated that it mitigates vulnerabilities identified by using a layered approach consisting of multiple technologies to detect and prevent compromise. Nevertheless, as stated in the report, GAO should take steps to ensure that these vulnerabilities are remediated in a timely manner, as the risk of compromise from high and critical vulnerabilities increases the likelihood that they could be used as part of an attack on GAO systems.

GAO disagreed with the finding that a business impact analysis had not been fully developed in 2018, but our audit work shows that while business impact analysis activities had been undertaken, a formal business impact analysis had not been completed. We look forward to reviewing the completed business impact analyses that will be conducted as part of GAO’s COOP update in 2020.

Fully implementing our recommendations will help to improve GAO’s information security program and provide additional assurance that critical data is protected in accordance with GAO’s information security goals.

Appendix I: Objective, Scope, and Methodology

OIG regularly assesses GAO's compliance with FISMA requirements. This report represents our assessment for fiscal year 2018. Specifically, our objective was to measure GAO's performance against select FISMA reporting metrics. The FISMA reporting metrics we used were from the following five categories of controls: (1) risk management, (2) configuration management, (3) contingency planning, (4) security training, and (5) information system continuous monitoring. We selected these specific metrics using a risk based approach, taking into account areas where GAO has previously experienced challenges. We did not assess the maturity of GAO's information security against the reporting metrics in the categories above.

To assess GAO's performance, we identified key information security criteria including best practices contained in the National Institute of Standards and Technology (NIST) guidance for implementing a security and privacy program. NIST special publications (SP) that were used as sources of criteria were:

- Managing Information Security Risk: Organization, Mission, and Information System View, SP 800-39
- Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, Revision 4
- Contingency Planning Guide for Federal Information Systems, SP 800-34

To review GAO's ability to manage cybersecurity risk, we selected FISMA reporting metrics related to the development of a risk management program where weaknesses had previously been identified but current data was not available. These areas included systems inventory, supply chain management, and remediation of identified vulnerabilities. We assessed GAO's:

- Risk management framework by reviewing key agency documents such as the enterprise risk management plan, performance plan, and budgetary documentation provided to Congress. Additionally, we interviewed agency officials who are knowledgeable about the GAO risk management program and its implementation.
- Asset management by reviewing the agency's enterprise architecture inventory and compared that to the systems inventory maintained by ISTS. We discussed discrepancies with ISTS so that we could better understand them.
- Contracting process by reviewing standard operating procedures which document GAO procedures for standard contract clauses. We also interviewed agency officials about language in the contracts and provided them with the opportunity to provide any additional language not originally reviewed.

In looking at GAO's implementation of system protections we selected FISMA reporting metrics related to the implementation of where weaknesses had previously been identified but current data was not available. We assessed GAO's:

- Remediation of vulnerabilities by reviewing vulnerability scanning reports created during September 2018. We reviewed these reports, removing duplicate hosts and vulnerabilities, to determine the number of vulnerabilities that were open at the end of FY 2018. To determine the days overdue we calculated the number of days since the vulnerability was overdue until the end of FY 2018 as that was the scope

of our audit. We also reviewed documentation related to GAO vulnerability remediation policies and interviewed GAO personnel with responsibilities for remediating and tracking vulnerabilities.

- Change management process by reviewing a list of changes that GAO processed during FY 2018 and selected all vulnerabilities categorized as Normal-Time Sensitive or Emergency. We then reviewed these vulnerabilities to see if they had been reviewed and approved by a member of ISSG. We also reviewed documentation related to GAO's change control process.
- Baseline configuration status by reviewing GAO's tracking sheet for baseline configurations to determine the current status of all environments that GAO has determined need a baseline configuration. We also interviewed agency officials about overdue baseline configurations to determine what part of the management process resulted in their being overdue.
- Security and awareness training by selecting all individuals who were recorded in GAO's training management system as having taken the security and awareness training. We then compared this list to all users who had active network accounts during FY 2018. We also reviewed a 2018 phishing exercise assessment to determine whether actions taken by GAO aligned with NIST guidance. We reviewed identified discrepancies with GAO personnel who are responsible for administering the training and reviewed GAO policies and procedures on employees taking security awareness training.

In order to examine GAO's ability to recover systems following a disaster we selected FISMA reporting metrics related to the development of information systems contingency plans. We assessed GAO's:

- Policies and procedures for conducting contingency plan testing and interviewed GAO personnel with responsibilities for reviewing and approving changes.
- Development of information system recovery plans by reviewing GAO information systems contingency plans for all systems and discussed and discrepancies with relevant GAO staff. We also reviewed GAO orders and policies on the development of information systems contingency plans.
- Use of business impact analyses by interviewing GAO staff members who are responsible for overseeing the Continuity of Operations Planning process including the development of business impact analyses. We also reviewed GAO policies and procedures for conducting business impact analyses.

We conducted this performance audit from December 2018 through September 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the U.S. Government Accountability Office

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Memorandum

Date: September 24, 2019

To: Adam R. Trzeciak
Inspector General
Office of Inspector General (OIG)

From: Howard M. Williams Jr.
Chief Information Officer

Subject: Information Security Review of GAO's Program and Practices for Fiscal Year 2018

Thank you for the opportunity to comment on your draft report on GAO's information security program. GAO is firmly committed to cybersecurity risk management and follows the Cybersecurity Framework (CFS) developed by the National Institute of Science and Technology (NIST) to ensure alignment of GAO's business needs to cybersecurity risk management. GAO has already mitigated and/or implemented corrective actions for many of the issues identified within this report.

One of the principal benefits of implementing the NIST cybersecurity framework is a strong security architecture capable of mitigating many of the risks associated with operating information technology (IT) networks.

GAO has a strong underlying infrastructure and employs a layered, multi-faceted approach to IT security that encompasses the NIST CFS core functions. The risk mitigation benefit of these security measures is taken into account when GAO makes decisions regarding security investments and operations. Examples of risk-based decisions include the remediation of vulnerabilities, completion of baseline configurations, and supply chain risk.

As a matter of practice, GAO takes its responsibility to secure its assets seriously. In 2018, we hired a recognized industry leader in IT security to perform an independent, third-party maturity assessment of our IT security program. This review identified numerous strengths associated with data protection; access management; host and endpoint protection; and application, database, and mobile protection, while also identifying areas for future improvement. GAO is addressing the few issues identified in this review.

While all risks cannot be eliminated, based on the external assessment, the OIG's FISMA reports, and our own cybersecurity program based on continuous process improvement, GAO's security program lowers IT vulnerability to a reasonable level. In addition, GAO has already corrected many of the issues identified in this report.

Recommendation 1: *In order to ensure a complete and actionable cybersecurity risk management program, finalize a key input to GAO's Enterprise Risk Management Strategy, specifically the risk appetite statement including risk tolerances.*

GAO has established a risk-based culture and reliable, effective risk management processes. GAO manages the agency using a risk-based approach focused on cost and, complexity. GAO's risk appetite and risk tolerance are currently reflected throughout the Agency's various policies and procedures and is consistent with guidance in OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. As part of the legislative branch, GAO is not subject to OMB guidance; but follows the spirit of Circular A-123 as a leading practices agency. While OMB Circular A-123 does not require a formal risk appetite statement, GAO plans to determine how to meet this element.

Recommendation 2: *Ensure that all entries in GAO's system inventory have been reviewed to determine if an impact assessment is needed and that assessments are performed as appropriate.*

As previously stated GAO is firmly committed to and follows the Cybersecurity Framework (CFS) developed by NIST to ensure alignment of business needs to cybersecurity risk management as well as taking the independent maturity risk assessment seriously.

Legacy systems are undergoing a systematic security review to ensure the appropriate level of protection for the system or data is implemented. To complement this review process, all legacy systems are protected as a result of the cybersecurity measures implemented by GAO. Any system placed on the GAO network automatically gains nearly all of these controls since underlying infrastructure and security measures are already interfacing with a system on the network (a system security assessment consists of a review of over 700 individual controls).

The implementation of these controls significantly reduces the risk to these systems and applications.

Recommendation 3: *Update standard operating procedures to ensure that standard contract language for security aligns with NIST recommendations as appropriate.*

GAO regularly reviews security needs including security requirements already built in to all GAO IT contracts as part of the statement of work. These requirements stipulate that vendors follow GAO's Information Systems and Technology Services (ISTS) unit's standard operating and security procedures (SOPs) and contain considerably more detailed language than general standardized contract language. While we believe the GAO contracting process does effectively mitigate supply chain risk, we will add the language requested by the OIG.

Page 2

Recommendation 4: *Take steps to ensure that identified vulnerabilities are remediated within prescribed time frames.*

The vulnerability scores reported in OIG's review are base scores that have not been adjusted to account for the mitigating measures that GAO implements as part of its cybersecurity risk management program. The scoring system provides a raw-risk score premised on full and open access to a system without any determination that mitigating factors reduce the risk.

Cybersecurity risk management cannot rely on a single technology or process to provide the full range of protections to mitigate the plethora of threats that abound across the internet. Vulnerability management is just a single aspect of GAO's entire process that supports the breadth of protections needed for GAO's information systems and data; which is why the Agency utilizes a layered approach that consists of security solutions for network access, intrusion detection/intrusion prevention, host-based protection, firewall protection, and network monitoring across GAO systems. GAO identifies weaknesses in technology working with government and industry partners, validates in-use technology risk, and mitigates risk using a multi-faceted, robust, layered approach to IT security that is consistent with the NIST CSF and other risk management guidance. In addition, GAO mitigates risk by the virtual desktop infrastructure (VDI) used at GAO which is updated daily.

Together, the VDI environment and these layers of protection mitigate the issues and reduce risk of compromise as identified by OIG in this report.

Recommendation 5: *Ensure that baseline configurations for all identified environments have been documented and approved.*

ISTS has an established procedure for introducing technology into the environment so that when new systems come online at GAO, they already have baseline configurations developed before being placed in production. Complete baseline configurations for some legacy systems are in progress or the systems are being retired.

ISTS has implemented automation and standard system templates used for the implementation of baseline configurations for technology. These procedures support a baseline standard for implementing the platform technology that maintains all of our applications. The use of virtual environments has solidified our ability to deploy standard baseline configurations for technologies that are used across our datacenter. The combination of automation, baseline templates, and virtualization has ensured a consistent approach to technology deployments across GAO. In addition we updated our SOPs for documenting emergency changes so that it is available to external reviewers.

In addition, GAO utilizes a defense-in-depth layered security architecture that significantly reduces the risk of a system weakness being exploited by an external threat. This architecture follows NIST guidance and consists of two-factor authentication for network access, intrusion protection/detection technologies; anti-malware/anti-virus protection, firewalls to screen network traffic and detect/block malicious traffic and network monitoring technologies that provide both an alert and blocking capability. In addition to these barriers, GAO mitigates risk by the virtual desktop infrastructure (VDI) used at GAO.

Page 3

Recommendation 6: *Ensure that contingency planning testing accurately reflects the ability of GAO to recover mission critical systems in the event of a disaster.*

Since the time of this review ISTS has improved its disaster recovery planning and documented it in both an Information Systems Contingency Plan (ISCP) and GAO's Disaster Recovery Plan (DRP). GAO held a contingency planning exercise in January 2019, and will be doing so annually going forward. Moreover, GAO's Incident Response Plan was identified as a strength in the independent maturity assessment conducted in fall 2018.

Recommendation 7: *Document and approve a contingency plan for the ARM Data Facility.*

Contingency planning for the ARM Data Facility does exist and we agree that the plans and procedures could be more formally documented in a master contingency planning document. The ARM Data Facility backs up all critical data to tape on a defined schedule and is available to mission teams in the event of a disaster.

Recommendation 8: *Complete business impact analysis for IT systems and update contingency plans where necessary to ensure that business needs are met in the event of a disaster.*

In 2018, GAO conducted a business process analysis and business impact analyses to support contingency planning decisions based in GAO's Continuity of Operations Plan (COOP). GAO has designated Mission Essential Functions which identify systems that are essential to GAO's business in an emergency setting. These are delineated in both the COOP and GAO's Disaster Recovery Plan. Plans are underway for review and update of COOP in 2020, which will include detailed business impact analyses.

Cc: Karl Maschino
Paul Johnson
Bill Anderson
Chuck Gepford
Dave Sadnavitch
Jennifer Ashley
Adebiyi Adesina

Text of Appendix II: Appendix II: Comments from the U.S. Government Accountability Office

Page 1

Memorandum

September 24, 2019 Adam R. Trzeciak

Inspector General.

Office of Inspector General (OIG)

Howard M. Williams Jr.

Chief Information Officer

Information Security Review of GAO's Program and Practices for Fiscal Year 2018

Thank you for the opportunity to comment on your draft report on GAO's information security program. GAO is firmly committed to cybersecurity risk management and follows the Cybersecurity Framework (CFS) developed by the National Institute of Science and Technology (NIST) to ensure alignment of GAO's business needs to cybersecurity risk management. GAO has already mitigated and/or implemented corrective actions for many of the issues identified within this report.

One of the principal benefits of implementing the NIST cybersecurity framework is a strong security architecture capable of mitigating many of the risks associated with operating information technology (IT) networks.

GAO has a strong underlying infrastructure and employs a layered, multi-faceted approach to IT security that encompasses the NIST CFS core functions. The risk mitigation benefit of these security measures is taken into account when GAO makes decisions regarding security investments and operations. Examples of risk-based decisions include the remediation of vulnerabilities, completion of baseline configurations, and supply chain risk.

As a matter of practice, GAO takes its responsibility to secure its assets seriously. In 2018, we hired a recognized industry leader in IT security to perform an independent, third-party maturity assessment of our IT security program. This review identified numerous strengths associated with data protection; access management; host and endpoint protection; and application, database, and mobile protection, while also identifying areas for future improvement. GAO is addressing the few issues identified in this review.

While all risks cannot be eliminated, based on the external assessment, the OIG's FISMA reports, and our own cybersecurity program based on continuous process improvement, GAO's security program lowers IT vulnerability to a reasonable level. In addition, GAO has already corrected many of the issues identified in this report.

Page 2

Recommendation, 1: In order to ensure a complete and actionable cybersecurity risk management program, finalize a key input to GAO's Enterprise Risk Management Strategy, specifically the risk appetite statement including risk tolerances.

GAO has established a risk-based culture and reliable, effective risk management processes. GAO manages the agency using a risk-based approach focused on cost and, complexity. GAO's risk appetite and risk tolerance are currently reflected throughout the

Agency's various policies and procedures and is consistent with guidance in 0MB Circular A- 123, Management's Responsibility for Enterprise Risk Management and Internal Control. As part of the legislative branch, GAO is not subject to 0MB guidance; but follows the spirit of Circular A-123 as a leading practices agency. While 0MB Circular A-123 does not require a formal risk appetite statement, GAO plans to determine how to meet this element.

Recommendation 2: Ensure that all entries in GAO's system inventory have been reviewed to determine if an impact assessment is needed and that assessments are performed as appropriate.

As previously stated GAO is firmly committed to and follows the Cybersecurity Framework (CFS) developed by NIST to ensure alignment of business needs to cybersecurity risk management as well as taking the independent maturity risk assessment seriously.

Legacy systems are undergoing a systematic security review to ensure the appropriate level of protection for the system or data is implemented. To complement this review process, all legacy systems are protected as a result of the cybersecurity measures implemented by GAO. Any system placed on the GAO network automatically gains nearly all of these controls since underlying infrastructure and security measures are already interfacing with a system on the network (a system security assessment consists of a review of over 700 individual controls).

The implementation of these controls significantly reduces the risk to these systems and applications.

Recommendation 3: Update standard operating procedures to ensure that standard contract language for security aligns with NIST recommendations as appropriate.

GAO regularly reviews security needs including security requirements already built in to all GAO IT contracts as part of the statement of work. These requirements stipulate that vendors follow GAO's Information Systems and Technology Services (ISTS) unit's standard operating and security procedures (SOPs) and contain considerably more detailed language than general standardized contract language. While we believe the GAO contracting process does effectively mitigate supply chain risk, we will add the language requested by the OIG.

Page 3

Recommendation 4: Take steps to ensure that identified vulnerabilities are remediated within prescribed time frames.

The vulnerability scores reported in OIG's review are base scores that have not been adjusted to account for the mitigating measures that GAO implements as part of its cybersecurity risk management program. The scoring system provides a raw-risk score premised on full and open access to a system without any determination that mitigating factors reduce the risk.

Cybersecurity risk management cannot rely on a single technology or process to provide the full range of protections to mitigate the plethora of threats that abound across the internet.

Vulnerability management is just a single aspect of GAO's entire process that supports the breadth of protections needed for GAO's information systems and data; which is why the Agency utilizes a layered approach that consists of security solutions for network access, intrusion detection/intrusion prevention, host-based protection, firewall protection, and network monitoring across GAO systems. GAO identifies weaknesses in technology working with government and industry partners, validates in-use technology risk, and mitigates risk using a multi-faceted, robust, layered approach to IT security that is consistent with the NIST CSF and other risk management guidance. In addition, GAO mitigates risk by the virtual desktop infrastructure (VOi) used at GAO which is updated daily.

Together, the VOi environment and these layers of protection mitigate the issues and reduce risk of compromise as identified by OIG in this report.

Recommendation 5: Ensure that baseline configurations for all identified environments have been documented and approved.

ISTS has an established procedure for introducing technology into the environment so that when new systems come online at GAO, they already have baseline configurations developed before being placed in production. Complete baseline configurations for some legacy systems are in progress or the systems are being retired.

ISTS has implemented automation and standard system templates used for the implementation of baseline configurations for technology. These procedures support a baseline standard for implementing the platform technology that maintains all of our applications. The use of virtual environments has solidified our ability to deploy standard baseline configurations for technologies that are used across our datacenter. The combination of automation, baseline templates, and virtualization has ensured a consistent approach to technology deployments across GAO. In addition we updated our SOPs for documenting emergency changes so that it is available to external reviewers.

In addition, GAO utilizes a defense-in-depth layered security architecture that significantly reduces the risk of a system weakness being exploited by an external threat. This architecture follows NIST guidance and consists of two-factor authentication for network access, intrusion protection/detection technologies; anti-malware/anti-virus protection, firewalls to screen network traffic and detect/block malicious traffic and network monitoring technologies that provide both an alert and blocking capability. In addition to these barriers, GAO mitigates risk by the virtual desktop infrastructure (VOi) used at GAO.

Page 4

Recommendation 6: Ensure that contingency planning testing accurately reflects the ability of GAO to recover mission critical systems in the event of a disaster.

Since the time of this review ISTS has improved its disaster recovery planning and documented it in both an Information Systems Contingency Plan (ISCP) and GAO's Disaster Recovery Plan (DRP). GAO held a contingency planning exercise in January 2019, and will be doing so annually going forward. Moreover, GAO's Incident Response

Plan was identified as a strength in the independent maturity assessment conducted in fall 2018.

Recommendation 7: Document and approve a contingency plan for the ARM Data Facility.

Contingency planning for the ARM Data Facility does exist and we agree that the plans and procedures could be more formally documented in a master contingency planning document. The ARM Data Facility backs up all critical data to tape on a defined schedule and is available to mission teams in the event of a disaster.

Recommendation 8: Complete business impact analysis for IT systems and update contingency plans where necessary to ensure that business needs are met in the event of a disaster.

In 2018, GAO conducted a business process analysis and business impact analyses to support contingency planning decisions based in GAO's Continuity of Operations Plan (COOP). GAO has designated Mission Essential Functions which identify systems that are essential to GAO's business in an emergency setting. These are delineated in both the COOP and GAO's Disaster Recovery Plan. Plans are underway for review and update of COOP in 2020, which will include detailed business impact analyses.

Cc: Karl Maschino

Paul Johnson Bill Anderson Chuck Gepford Dave Sadnavitch Jennifer Ashley Adebiyi Adesina

Appendix III: OIG Contact and Staff Acknowledgments

OIG Contact

Adam R. Trzeciak, (202) 512-5748 or trzeciaka@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Mary Arnold Mohiyuddin (Assistant Inspector General for Audit), Thomas J. Johnson (Engagement Manager), and Adriana Pukalski (Legal Counsel) made major contributions to this report. Other key contributors include Melanie H. P. Fallow and Cynthia Taylor.

Appendix IV: Report Distribution

U.S. Government Accountability Office

Gene L. Dodaro – Comptroller General
Katherine A. Siggerud – Chief Operating Officer
Karl J. Maschino – Chief Administrative Officer/Chief Financial Officer
Thomas H. Armstrong – General Counsel
Howard M. Williams, Jr. – Chief Information Officer
Terrell G. Dorn – Managing Director, Infrastructure Operations
Orice Williams Brown – Managing Director, Congressional Relations
Chuck Young – Managing Director, Public Affairs
William L. Anderson – Controller/Deputy Chief Financial Officer
Adebiyi A. Adesina – Special Assistant to the Controller

GAO Audit Advisory Committee

GAO Congressional Oversight Committees

OIG Mission

Our mission is to protect GAO's integrity through audits, investigations, and other work focused on promoting the economy, efficiency, and effectiveness in GAO programs and operations, and to keep the Comptroller General and Congress informed of fraud and other serious problems relating to the administration of GAO programs and operations.

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud and other serious problems, abuses, and deficiencies relating to GAO programs and operations, you can do one of the following (anonymously, if you choose):

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Visit https://OIG.alertline.com.

Obtaining Copies of OIG Reports and Testimonies

To obtain copies of OIG reports and testimonies, go to GAO's website: www.gao.gov/about/workforce/ig.html or https://www.oversight.gov/reports

.